UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/556,068	04/21/2000	Sai V. Allavarpu	5181-48400	6894

7590 11/19/2003

Robert C Kowert
Conley Rose and Tayon P C
P O Box 398
Austin, TX 78767-0398

EXAMINER	
PATEL, HARESH N	
ART UNIT	**PAPER NUMBER**
2126	8

DATE MAILED: 11/19/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/556,068	ALLAVARPU ET AL.	
	Examiner	Art Unit	
	Haresh Patel	2126	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-57 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-57 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-57 are presented for examination.

Specification

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: "Secure access to the Telecom Network Management devices using a configurable platform-independent CORBA gateway".

Drawings

3. Figure 1b should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 20 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker et. al. 6,363,421 (Hereafter Barker) in view of Grantges, Jr. 6,324,648 (Hereafter Grantges).

6. As per claims 1, 20 and 39, Barker teaches the following:

a network management system comprising (e.g., a management computer is connected to an element management system server through a special communication link including a computer internet, col.1, lines 27-30),

a network management method comprising (e.g., a method is provided for remotely managing a plurality of network element of a telecommunications network, col. 1, lines 24-30),

a carrier medium comprising program instructions for network management, wherein the program instructions are computer-executable to perform:

a gateway (e.g., an element management server) which is coupled to one or more managed objects (e.g. at least one of the plurality of network elements is also coupled to the element management server through the computer internet, e.g., col. 1, lines 29-36) and which is configured to deliver events generated by the managed objects to one or more managers (e.g., The object server provides a way for client applications to receive information about network elements and other associated managed objects and to issue commands that are executed on the network element. To accomplish these functions, the object server provides the following services: (1) client session registration, (2) event distnbution and screening, (3) command management, (4) SNMP mediation, and (5) services specific to each managed object class, col. 10, line 51 – col. 17, line 59), or to deliver requests generated by the managers to the one or more managed objects (e.g., The object server provides a way for client applications to receive

information about network elements and other associated managed objects and to issue commands that are executed on the network element. To accomplish these functions, the object server provides the following services: (1) client session registration, (2) event distnbution and screening, (3) command management, (4) SNMP mediation, and (5) services specific to each managed object class, col. 10, line 51 – col. 17, line 59); and

a platform-independent interface to the gateway (e.g., CORBA will serve as the IPC for functions residing on the server, thereby eliminating any platform-specific IPC from the implementation, col. 4, lines 37-55), wherein the gateway is configurable to communicate with the managers through the platform-independent interface to deliver the events or requests (e.g., The element management system server 32 executes applications to serve information to clients via CORBA middleware. CORBA will serve as the IPC for functions residing on the server, thereby eliminating any platform-specific IPC from the implementation, and providing for distribution of functionality to multiple processors if needed in the future for performance, col. 4, lines 1 – 67),

Barker teaches user session's manager to maintain a list of active client sessions and applications. Barker discloses that in subsequent releases, the service object will provide user access security on a network-element and operation basis, e.g., figure 16 and figure 17. Barker teaches an object identifier that uniquely identifies a specific managed object instance and to identify the specific managed object instance that generated the event, validate client security and permissions. Barker teaches the Event Distributor is responsible for filtering and routing of all events in the system, col. 1, line 7 – col. 4, line 64. Barker also teaches the Filter object

containing a specification describing events to be delivered to the client, e.g., col. 13, line 48 – col. 17, line 58.

However Barker does not specifically show object-level access control between the managers and the managed objects.

As per claims 1, 20 and 39, Grantges teaches the following:

wherein the gateway is configurable to provide object-level access control between the managers and the managed objects to receive the events from or to send the requests to the managed objects, determine on a managed object level whether or not the manager application is allowed to receive an event generated by a managed object or to send a request to the managed object as a function of the identity of the user of the manager application, whereby access for the manager application to receive the event or send the request is approved or denied for said managed object, delivering the event to the manager application or the request to the managed object if the manager access is approved (e.g., A computer system provides authenticated access for a client computer over an insecure, public network to one of a plurality of destination servers on private, secure network, through the use of a client-side X.509 digital certificate. A firewall is disposed between the insecure, public network and the private network. A demilitarized zone (DMZ) proxy server intercepts messages destined for the destination servers, and forwards the intercepted messages through the firewall to a gateway on the private network. The gateway is configured to create a cookie, based on the selection of one of a several applications available on the private network. The cookie contains an identifier sufficient to identify the destination server corresponding to the selected application. Messages from the client computer include the cookie. The gateway processes the cookie and appends the identifier on a destination URL

portion of the messages for routing. An alternate computer system authenticates a user of a remote client computer on the insecure network side of the firewall using a user identification and password, abstract).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Barker with the teachings of Grantges in order to facilitate a secure access to the Telecom Network Management devices using a configurable platform-independent gateway.

7. Claims 2-4, 21-23 and 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker in view of Grantges.

8. As per claims 2-4, 21-23 and 40-42, Barker teaches the following:

the gateway is configurable to determine whether each of the managers is authorized to communicate with each of the managed objects (e.g., the server supports basic server authentication, and can be enhanced to support SSL (Secure Socket Layer) if encryption of the browser to server connection is required. Secure administrator administration of web server including administration of the client name and password for access control, col. 8, lines 31-54),

the gateway is configurable to authenticate the managers to receive the events from or to send the requests to the managed objects as a function of the identity of the managed object objects (e.g., the server supports basic server authentication, and can be enhanced to support SSL (Secure Socket Layer) if encryption of the browser to server connection is required. Secure administrator administration of web server including administration of the client name and password for access control, col. 8, lines 31-54),

the gateway is configurable to authenticate the managers to receive the events or send the requests as a function of user IDs entered by users of the managers objects (e.g., the server supports basic server authentication, and can be enhanced to support SSL (Secure Socket Layer) if encryption of the browser to server connection is required. Secure administrator administration of web server including administration of the client name and password for access control, col. 8, lines 31-54).

9. Claims 5, 24 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker in view of Grantges.

10. As per claims 5, 24 and 43, Barker teaches the following:

the events or requests are delivered by the gateway through the platform-independent interface according to Internet Inter-Object Protocol (IIOP) (e.g., the Orbix Naming Service daemon provides symbolic lookup of servers on the network and is necessary to support the IIOP protocol, col. 9, lines 15-19).

11. Claims 6-7, 25-26 and 44-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker in view of Grantges.

12. As per claims 6-7, 25-26 and 44-45, Barker teaches the following:

the platform-independent interface to the gateway is expressed in an interface definition language (e.g., The element management system server 32 executes applications to serve information to clients via CORBA middleware. CORBA will serve as the IPC for functions residing on the server, thereby eliminating any platform-specific IPC from the implementation,

and providing for distribution of functionality to multiple processors if needed in the future for performance. Communication between the element management system and the managed elements is via SNMP, the EMAPI 55 is implemented utilizing an industry standard object management group interface description language (IDL), col. 33, line 3 – col. 43, line 34), and wherein the interface definition language comprises a language for defining interfaces to the managed objects across a plurality of platforms and across a plurality of programming languages (e.g., IDL is used to describe any resource or service a server component wants to expose to its clients without regard to its implementation language or operating system, col. 33, line 3 – col. 43, line 34, figure 15),

the interface definition language comprises OMG IDL (e.g., object management group (OMG) IDL, col. 7, lines 1-30).

13. Claims 8-9, 27-28 and 46-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker in view of Grantges.

14. As per claims 8-9, 27-28 and 46-47, Barker teaches the following:

the managed objects comprise one or more objects corresponding to a telephone network (e.g., a management computer associated with an element management system client is connected to a network element and element management system client through a public telephone network (PSTN), col. 3, lines 47 – 54, figure 1A),

the managed objects comprise an object corresponding to a telecommunications device (e.g., method for computer internet remote management of a telecommunication network element, title).

15. Claims 10-15, 29-34 and 48-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker in view of Grantges.

16. As per claims 10-15, 29-34 and 48-53, Barker teaches the following:

the gateway is configurable to provide security audit trails (e.g., Security, this functionality provides a method of client based access control of network elements, maintenance units and operations on network elements/maintenance units, the server retrieves the client record from local data services, col. 30, lines 44-63),

the gateway providing security audit trails comprises the gateway providing access to a logging service (e.g., a client application must register with the server by providing identification of the client host, port, client , and a password, col. 30, lines 44-63),

the logging service is operable to log an ID of a user that receives each event or sends each request (e.g., a client application must register with the server by providing identification of the client host, port, client , and a password, in any case, all client requests are validated at the server, col. 30, lines 44-63, A log file containing the IP address and the URL referenced. This is used to examine access patterns and detect and trace access from unauthorized sources. Web page access control based on client name and password. The server supports basic server authentication, and can be enhanced to support SSL (Secure Socket Layer) if encryption of the browser to server connection is required. Secure administrator administration of web server including administration of the client name and password for access control, col. 7 – line 38 – col. 20, line59),

the logging service is operable to log an ID of the managed object that is the source of each event or the target of each request (e.g., a client application must register with the server by providing identification of the client host, port, client , and a password, in any case, all client requests are validated at the server, col. 30, lines 44-63, A log file containing the IP address and the URL referenced. This is used to examine access patterns and detect and trace access from unauthorized sources. Web page access control based on client name and password. The server supports basic server authentication, and can be enhanced to support SSL (Secure Socket Layer) if encryption of the browser to server connection is required. Secure administrator administration of web server including administration of the client name and password for access control, col. 7 – line 38 – col. 20, line59),

the logging service is operable to log a time at which each event or request is generated (e.g., Event configuration file defines which events are to be logged locally , col. 31, lines 51-65, an event header contains information, time of the event, col. 41, lines 62-66, A log file containing the IP address and the URL referenced. This is used to examine access patterns and detect and trace access from unauthorized sources. Web page access control based on client name and password. The server supports basic server authentication, and can be enhanced to support SSL (Secure Socket Layer) if encryption of the browser to server connection is required. Secure administrator administration of web server including administration of the client name and password for access control, col. 7 – line 38 – col. 20, line59),

However Barker does not specifically show some of the limitations of claims 10-15, 29-34 and 48-53.

As per claims 10-15, 29-34 and 48-53, Grantges teaches the following:

the gateway is configurable to provide security audit trails (e.g., FIG. 4A shows several "cookies" created by gateway proxy server 40: an authentication cookie 90, an applications list cookie 92, and a selected-application cookie 94. A cookie message is given to a client (e.g., a web browser) by a server. The client will cache the cookie, and store the cookie in a file on the client computer 22 if the cookie is a so-called "persistent" cookie, col. 3, line 61 – col. 16, line 10, an administrative interface (not shown) is provided on authorization server 46, and allows any individual classified as an "admin" user to execute certain functions. These functions fall into three main categories: (i) user administration; (ii) application administration; and, (iii) reports. For example, "admin" users may add or delete users, provide for user update/maintenance, provide user searches, add an application, attend to application maintenance, provide login access reports, provide inactive and/or expired user reports, and provide a user list report, col. 3, line 61 – col. 16).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Barker with the teachings of Grantges in order to facilitate a secure access to the Telecom Network Management devices using a configurable platform-independent gateway.

17. Claims 16-17, 35-36 and 54-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker in view of Grantges.

18. As per claims 16-17, 35-36 and 54-55, Barker teaches the following:

the requests comprise a query for information concerning one of the managed objects (e.g., Each agent must generate an acknowledgment trap in response to each command request

containing the originating session identifier and command sequence number along with an acknowledgment value indicating whether the command request is invalid or could not be processed, processed as requested with no further response, or in progress with additional response pending, col. 17, line 4 – col. col. 27, line 4),

the requests comprise a command to set one or more parameters of one of the managed objects (e.g., command type, object instance id, command qualifier, some commands may require additional argument, since each command block is defined separately, it is simple to implement additional arguments, col. 17, line 4 – col. col. 27, line 4).

19. Claims 18-19, 37-38 and 56-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker in view of Grantges.

20. As per claims 18-19, 37-38 and 56-57, Barker teaches the following:

the requests are converted from the interface definition language to a Portable Management Interface (PMI) format prior to delivery to the managed objects (e.g., SNMP Mediator 160 provides translation between the MIB ASN.1 format and the managed object notation used in this architecture, figure 3, FIG. 9 is a block diagram showing a network element, AP, service object and the data it contains and an ECP managed object using a protocol other than SNMP for communication),

the requests are converted from the interface definition language to a platform-specific format prior to delivery to the managed objects (e.g., SNMP Mediator 160 provides translation between the MIB ASN.1 format and the managed object notation used in this architecture, figure

3, FIG. 9 is a block diagram showing a network element, AP, service object and the data it contains and an ECP managed object using a protocol other than SNMP for communication).

Response to Amendments

21. Applicant's arguments with respect to claims 1-57 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

22. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Haresh Patel whose telephone number is (703) 605-5234. The examiner can normally be reached on Monday, Tuesday, Thursday and Friday from 10:00 am to 8:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee, can be reached at (703) 305-8498.

The appropriate fax phone number for the organization where this application or proceeding is assigned is (703) 306-5404.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Haresh Patel

November 1, 2003.

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100